Appl. No. 10/823,132
Amdt. dated December 23, 2008
Reply to office action of September 24, 2008

Amendments to the Claims

1-28. (Cancelled)

29. (Currently Amended) A method of operating a computing platform, the method comprising:

receiving a secured data product comprising an encrypted first portion of the data product and an unencrypted second portion of the data product, wherein said first portion of the data product comprises indices into data contained in the second portion of the data product, said encrypted first portion being unusable by the computing platform before decrypting said encrypted first portion and said unencrypted second portion being unusable by the computing platform before decrypting said encrypted first portion;

decrypting said encrypted first portion with a decryption key to obtain said indices into data contained in the second portion; and

executing an application program on the computing platform to use the data product including both the decrypted first portion and the second portion for an intended purpose, wherein to use the data product for said intended purpose said indices are used to obtain said data contained in the second portion of the data product, wherein said application program is not included with said data product, wherein said application program being installed on said computing platform prior to said step of receiving said secured data product.

30. (Previously Presented) The method of claim 29 wherein said first portion of the data product includes decompression parameters for the data product.

31. (Canceled)

32. (Previously Presented) The method of claim 29 wherein said first portion of the data product comprises global data pertaining to the data product as a whole.

33. (Previously Presented) The method of claim 29 wherein the data product further includes an encrypted authorization key and said method further comprises decrypting said encrypted authorization key to obtain verification information.

34. (Previously Presented) The method of claim 33 wherein said verification information comprises an ID code associated with a computing platform entitled to access the data product.

35. (Previously Presented) The method of claim 33 wherein said verification information comprises an ID code associated with a storage medium entitled to hold the data product.

36. (Previously Presented) The method of claim 33 wherein said verification information comprises an ID code associated with a user entitled to use the data product.

37. (Previously Presented) The method of claim 33 wherein said decrypting said authorization key provides said decryption key for decrypting said first portion of the data product.

38. (Currently Amended) A computing system comprising:

a processor;

a data storage medium coupled to said processor, the data storage medium holding a set of data comprising an encrypted first portion of a data product and an unencrypted second portion of the data product, wherein the first portion comprises critical data that enables use of the data product, wherein said critical data is not a decryption key, wherein the first portion of the data product being unusable by the computing platform before decrypting said encrypted first portion and the second portion of the data product being unusable before decrypting the first portion of the data product; and

a routine executable by the processor for decrypting the encrypted first portion of the data product, thereby enabling a program executable by said processor to use the data product including both the first portion and the second portion for an intended purpose, wherein said program is not included with said data product.

39. (Previously Presented) The system of claim 38 wherein said data product is a geographic database.

40. (Previously Presented) The system of claim 38 wherein said critical data includes decompression parameters for the data product.

41. (Previously Presented) The system of claim 38 wherein said set of data further comprises an encrypted authorization key.

42. (Previously Presented) The system of claim 41 further comprising a second routine executable by the processor for decrypting the encrypted authorization key to obtain verification information to validate use of the data product.

43. (Previously Presented) The system of claim 41 further comprising a second routine executable by the processor for decrypting the encrypted authorization key to obtain a decryption key for decrypting the first portion of the data product.

44. (Currently Amended) A data product stored on a medium comprising:

an encrypted first portion; and

an unencrypted second portion, wherein said first portion comprises critical data that when decrypted enables a program executed on a computing platform to use the data product including both said first portion and said second portion for an intended purpose, wherein said first portion comprises indices into data contained in the second portion of the data product,

wherein the encrypted first portion being unusable before decrypting said encrypted first portion and the unencrypted second portion of the data product not being usable before decrypting the encrypted first portion of the data product to obtain the indices, said program is not included with said data product.

45. (Previously Presented) The data product of claim 44 wherein said data product comprises a geographic database.

46. (Canceled).

47. (Previously Presented) The data product of claim 44 wherein said critical data comprises global data pertaining to said data product as a whole.

48. (Previously Presented) The data product of claim 44 wherein said encrypted first portion includes an authorization key.

49. (Currently Amended) A method for securely providing a database to a client, the method comprising:

dividing the database into a first portion and a second portion, the first portion comprising at least some critical data, the second portion not usable without the critical data in the first portion, wherein the critical data are selected from the group consisting of: decompression parameters, indices, and global data, wherein said critical data is not a decryption key;

encrypting the first portion of the database including the critical data;

sending to the client the encrypted first portion of the database, the unencrypted second portion of the database, and a key for decrypting the first portion of the database, wherein the first portion and the second portion of the database are not usable before decrypting the first portion.

50. (Canceled).